Information hiding techniques for infrared images: exploring the state-of-the art and challenges

Information Hiding Techniques for Infrared Images: exploring the state-of-the art and challenges

Victor Pomponiu*[a], Davide Cavagnino[b], Marco Botta[b], Hossein Nejati[a]
[a]Information Systems Technology and Design, Singapore University of Technology and Design, Somapah Road 8, Singapore, 487372;
[b]Department of Computer Science Universita degli Studi di Torino, Corso Svizzera 185, 10149, Torino, Italy

ABSTRACT

The proliferation of Infrared technology and imaging systems enables a different perspective to tackle many computer vision problems in defense and security applications. Infrared images are widely used by the law enforcement, Homeland Security and military organizations to achieve a significant advantage or situational awareness, and thus is vital to protect these data against malicious attacks. Concurrently, sophisticated malware are developed which are able to disrupt the security and integrity of these digital media. For instance, illegal distribution and manipulation are possible malicious attacks to the digital objects. In this paper we explore the use of a new layer of defense for the integrity of the infrared images through the aid of information hiding techniques such as watermarking. In this context, we analyze the efficiency of several optimal decoding schemes for the watermark inserted into the Singular Value Decomposition (SVD) domain of the IR images using an additive spread spectrum (SS) embedding framework. In order to use the singular values (SVs) of the IR images with the SS embedding we adopt several restrictions that ensure that the values of the SVs will maintain their statistics. For both the optimal maximum likelihood decoder and sub-optimal decoders we assume that the PDF of SVs can be modeled by the Weibull distribution. Furthermore, we investigate the challenges involved in protecting and assuring the integrity of IR images such as data complexity and the error probability behavior, i.e., the probability of detection and the probability of false detection, for the applied optimal decoders. By taking into account the efficiency and the necessary auxiliary information for decoding the watermark, we discuss the suitable decoder for various operating situations. Experimental results are carried out on a large dataset of IR images to show the imperceptibility and efficiency of the proposed scheme against various attack scenarios.

Keywords: **authentication; image integrity; information hiding; infrared images; optimum decoding and detection; Singular Value Decomposition (SVD); spread spectrum embedding; security;**

1. INTRODUCTION

Nowadays, the application of infrared thermal imaging technology in remote sensing, healthcare and defense has continually achieving significant importance. Infrared (IR) images are represented as gray-scale images for which the gray value of each pixel denotes the temperature field radiated from the objects. However, the statistics of IR images is different from those of natural images which have been extensively studied [1]. By computing the distribution of the pixels and their statistics for this image modality will enable low-level vision applications that can lead to significant advances in computer vision, as well as further our understanding of biological vision systems.

Due to the rising dependence on digital media and development of network technology, it is convenient to communicate and adopt IR images, but it also allows a malicious attacker to access, edit and copy the content without restriction, which reduces the value of IR images. Thus, techniques which provide the ability to communicate secretly and the capacity to protect copyrighted IR content are continually achieving significant importance.

One common information hiding technique for digital right protection is digital watermarking [2], where a particular signal, which determines the ownership, is embedded into the host media content without significantly deteriorating the perceptual quality of the original media. Contrary to encryption, watermarked media can still be perceptually used while remaining protected, and thus watermarking can offer post-deployment security of digital media content.

It is worth mentioning that, despite the popularity of watermarking techniques, effective digital protection is extremely challenging and currently there is no commonly accepted technical solution which is practically unbeatable when deployed to practical user settings [3]. By any means, watermarking techniques should only be considered as one important component of an overall protection system. Amongst the proposed schemes for watermark embedding, spread spectrum (SS) and quantization based methods [4, 5] are the two main broad categories.

In SS watermarking embedding, a multiplicative or additive watermark is merged with the host signal. The quantization based schemes are implemented by quantizing the host signal to the nearest lattice point. In this article, we focus on spread spectrum embedding schemes originally proposed by Cox et al. [2]. The watermark is detected at the receiver side without the original media content which, in this blind case, is treated as a noise source. The additive SS [6] watermarking spreads the watermark over the host signal uniformly while in multiplicative SS [7, 8], the watermark spreads according to the unreeling content of the host signal. To decrease the noise effect of the host signal in additive SS, Malvar and Florencio [9] proposed an improved spread spectrum (ISS) - a new modulation scheme which exploits the side information at the encoder to reduce the effect of host signal and increase the decoding performance [10]. Lately, the several embedding schemes have been proposed combining the SS and ISS schemes which employ the correlation between the host signal and the signature code (i.e., a binary sequence derived from a secret key) to improve the decoding performance [11].

Watermarking techniques ca be split in two main categories depending on their intended purpose: in the first category [12], the inserted watermark is used to communicate a specific hidden message (e.g., a binary secret message) that needs to be extracted with adequate decoding precision. In the other type of systems, the aim is to merely verify whether a particular embedded watermark (e.g., denoting the copyright information) is detected (presented) or not; thus, the inserted watermark does not transfer a secret message which must be accurately decoded. It is worth to point out that the two categories generate different detection (decoding) approach which serves different performance criteria [12].

Based on the above two categories of watermarking schemes, the watermark extraction types can be divided into: *watermark decoding* [12] for the case of decoding the embedded watermark (i.e., the hidden message) and *watermark detection* [13-16] for the case of detecting the presence of a specific watermark. Watermark detection and decoding problems are similar but they are employed for different goals and use different criteria. In watermark decoding, the hidden message should be extracted (decoded) with sufficient precision at the receiver side. The performance criterion used to measure the detection accuracy is the bit error rate and the watermark decoding problem can be formulated as minimizing the bit error rate. Instead, for watermark detection the detection criteria are usually based on Neyman-Pearson Theorem, that aims to maximize the probability of detection for a given probability of false alarm. Performance criterion like the true detection probability and the false alarm probability are applied for evaluating the watermark detector performance.

It important to note that a watermark detector does not implies a specific watermark decoder due to the fact that the watermark decoding problem uses a different hypotheses testing problem from the watermark detection problem. In case of the local optimum (LO) test different forms of the LO detector and the LO decoder are generated. Furthermore, maximum likelihood (ML) criterion has different interpretations for each watermark extraction type:

- For the ML watermark decoder is a Bayesian optimization approach that minimizes the probability of bit error when considering equal prior probability of the bit information (thus, assuming the decoding threshold to be 1);
- For the ML watermark detection solution is the detector based on the Neyman-Pearson theorem (the probability of false alarm is employed to compute the detection threshold).

The common goal of communicating secret messages using watermarking is to successfully insert and decode imperceptible watermarks which can be resistant against attacks. To reduce the decoding degradation against signal processing attacks and to exploit the properties of certain transform domain, the message can be embedded in different domains such as the Discrete Fourier Transform (DFT) [12,17], the discrete cosine transform (DCT) domain [18, 19], the discrete wavelet transform (DWT) domain [20, 21] and the Singular Value Decomposition (SVD) domain [22, 23].

Cox et al. introduced the first watermark decoder for the SS embedding, which extracts the inserted message using the correlation between the signature code and the received data. They showed that by making use of the probability density function (PDF) of the host signal the performance of watermark decoding could be significantly improved. Later, several other researchers proposed optimal ML decoders for additive SS in the DCT domain [24] and for multiplicative SS in the DFT domain [12].

In this paper, we concentrate our attention on watermark decoding, since we are interested in decoding the hidden message. We adopt a more realistic scenario, i.e., the blind watermark decoding, that assumes the original host image is not available at the receiver side. Therefore, we investigate the efficiency of blind decoding schemes for the watermark inserted into the SVD domain of the infrared host images using an additive SS embedding approach (i.e., the SS-SVD scheme). It is worth to point out that we assume the PDF of the components of the SVD transform (i.e., the singular values) can be modeled by the Weibull distribution.

The rest of the paper is organized as follows: Section 2 introduces the most relevant works related to information hiding for IR images. A short overview of the SVD and host probability distribution functions for the SVD domain are described in Section 3. In Section 4 the traditional additive SS embedding scheme is briefly reviewed for data hiding. The optimal ML decoder is derived in Section 5 and the corresponding bit-error-rate analysis is presented. The simulation results are demonstrated in Section 6 to validate the analysis. Finally, the discussions and concluding remarks are given in Section 7.

2. RELATED WORKS

There is a plethora of information hiding schemes that have been applied for the gray-scale and color images, but only few that are working with IR images. In this section we discuss the existing solution, in general non-blind and semi-blind, that have been proposed for watermarking IR images.

In [21] a non-blind watermarking scheme based on integer wavelet transform is proposed. In order to increase the security of the scheme the watermark (i.e., a binary logo image) is encrypted by a chaotic sequence (i.e., Logistic chaotic sequence [25]). The additive embedding of the secret information is done adaptively, by employing the just noticeable distortion [26], in perceptually significant mid and high frequency wavelet coefficients. The hierarchically detection was employed to recover the inserted watermark. Experimental results show that the algorithm can produce acceptable quality watermarked images and can ensure robustness against common signal processing operations. One of the issue of the algorithm is that it cannot recover the watermark even if the watermarked image did not undergo any modifications.

Zhao et al. [27] proposed a transform domain watermarking scheme, inspired from [18], which employs a blind IR-based decoding framework. The watermark message is inserted by modulating frequency components of the black plane of a printed CMYK image. It actually uses the SS embedder proposed by Cox et al [18]. The scheme works by first converting the input image, which could be in any format, into a CMYK (Cyan, Magenta, Yellow and Key) image for a printer device through a standard image path connecting both source and destination profiles. Secondly, the black plane is transformed to the DCT domain and certain coefficients are selected to convey the watermark information. To reduce the distortion due to the watermark insertion an adjustment step is applied on the other color planes, i.e., C, M and Y. The detection works by scanning a hardcopy of the watermarked image with an infrared scanner. The scanned image is then processed to accommodate the geometric distortions. In addition, the scanned image is corrected for the nonlinear relationship between infrared signals and black amounts. Finally, by using the encoding algorithm, the watermark is extracted from the infrared scanned image and compared without the original image to verify the presence of the watermark. The main advantages of the scheme are its ability to blind decoding and that it can reach less visual noise artifacts since the perceptible watermarking noise is still much lower than in many traditional methods.

In [28] the authors introduced a watermarking robust against re-recoding of videos displayed on screen by focusing a camcorder towards the screen and pressing the record button. Basically the idea is to use IR light of 870 nm to add noise to images displayed on a screen without it being detected by the human eye. The overcome the filtering attack applied on the video frames [29, 30], based on a short wavelength pass filter that bocks the IR signal while allowing short wavelength light to pass, the authors use a hardware equipment, i.e., IR LEDs bullet type and chip type with lens, attached on the displaying screen that can detect the IR light reflected off the filter by using the IR specular reflection properties of the filter. Therefore, in this manner the copy protection system identifies re-recording using digital camcorders equipped with a short wavelength pass filter.

3. THE SINGULAR VALUE DECOMPOSITION

One of the most interesting and important developments of linear algebra is the concept of Singular Value Decomposition (SVD) of matrices. Essentially, the SVD is a matrix factorization technique [31]. It is applicable to matrices with complex or real values and has been extensively applied in information retrieval, recommender systems and signal processing [23], like image compression, noise reduction or data hiding.

Let's consider $I_h \in \mathfrak{F}^{M\times N}$ as the host image that need to be watermarked and $\mathfrak{F}$ the image alphabet. In the case of a gray-scale image $\mathfrak{F} = \{0, 1, \ldots, 255\}$, while M and N denote the image size. We assume that $M = N$, although the obtained results can be extended to the general scenario when $M \neq N$. The singular value decomposition of the host image I_h is defined as:

$$\mathrm{SVD}(I_h) = [U^{M\times M}, \Delta^{M\times M}, V^{M\times M}], \tag{1}$$

where the diagonal components of the matrix Δ are the singular values (SVs) of I_h sorted in descending order, and the columns of U/V denotes the left/right singular vectors. Furthermore, U and V are unitary matrices, that means $U \cdot U^T = I^{M \times M}$, $V \cdot V^T = I^{M \times M}$, where $I^{M \times M}$ is the identity matrix. The SVs are related to the brightness (luminosity) of Ih while singular vectors describe its structural details, such as weak and strong edges, corners and shapes.

The host PDF for the SVD domain

To develop the optimal ML decoder the distribution of the singular values is necessary. Since the magnitude of the SVs is real and positive we choose the Weibull distribution to model their probability density function (PDF) as follows

$$f_X(x;\ \tau, \gamma) = \frac{\gamma}{\tau}\left(\frac{|x|}{\tau}\right)^{\gamma-1} \exp\left[-\left(\frac{|x|}{\tau}\right)^{\gamma}\right] u(x) \tag{2}$$

where $\gamma > 0$ is the shape parameter, $\tau > 0$ is the scale parameter and $u(\cdot)$ denotes the step function which returns one where its argument is positive and returns zero when its argument is negative.

4. THE SS-SVD EMBEDDING

The generic SS embedding framework can be described as follows: the host image I_h is split into $M/n \times M/n$ non-overlapping blocks of size $n \times n$ and then each block is transformed to the SVD domain. One bit of the message ($m_k \in \{\pm 1\}$, $k = 1, 2, \ldots, (M/n)^2$) is inserted in each block of the image.

A set of SVs coefficients of length $L \leq n^2$ is selected as the feature vector from each transformed block. To increase the security a signature sequence $\mathrm{s} = [s_1, s_2, \ldots, s_L]^T$ with $s \in \{\pm 1\}$ is used in conjunction with the inserted bit to obtain the watermark sequence. The selected feature vectors $x_k \in \mathrm{R}^L$, $k = 1, 2, \ldots, (M/n)^2$, $\mathrm{x} = [x_1, x_2, \ldots, x_L]^T$ are employed for watermark insertion as follows:

$$\mathrm{y} = \mathrm{x} + \mathrm{s} \cdot \alpha \cdot m_k, \tag{3}$$

where y is the watermarked vector of length L and α is the bit strength for embedding. Furthermore, the distortion due to the bit insertion is equal to:

$$D = \frac{1}{L} E\{|\mathrm{y} - \mathrm{x}|^2\} = \alpha^2 \tag{4}$$

The SVD domain imposes several limitations that affect the SS embedding procedure. The components of the feature vectors, i.e., the SVs of the each image block, should remain real and positive after embedding the watermark bit. In order to ensure these properties the SS embedding rule is adjusted as follows:

$$\mathrm{y} = \mathrm{x} + \mathrm{s} \cdot \alpha \cdot m_k + \theta, \tag{5}$$

where the vector $\theta = [\theta_1, \theta_2, \ldots, \theta_L]^T$ is employed to maintain the component of y positive. In particular, if $x_i + \mathrm{s}_i \cdot \alpha \cdot m_{i,k}$ is positive then the corresponding coefficient θ_i is set to zero. Instead, if $x_i + \mathrm{s}_i \cdot \alpha \cdot m_{ik}$ is negative then the coefficient θ_i is set to $-\mathrm{s}_i \cdot \alpha \cdot m_{ik}$ to obtain x_i positive. Therefore the vector θ is defined as:

$$\theta_i = \begin{cases} 0 & ,\ x_i + s_i \cdot \alpha \cdot m_{i,k} > 0 \\ -\mathrm{s}_i \cdot \alpha \cdot m_{i,k}, & x_i + s_i \cdot \alpha \cdot m_{i,k} < 0 \end{cases} \tag{6}$$

Basically, the embedding procedure makes the coefficients of the watermarked vector equal to x_i ($y_i = x_i$) if $\theta_i > 0$, which means that y_i will not hide any bit of the watermark. Another interesting aspect that emerges from (6) is that the watermarked coefficients decrease by increasing the watermarking strength α. Normally, the goal of this modified SS embedding approach is to create all the watermarked coefficients positive.

5. THE OPTIMAL ML DECODER IN THE SVD DOMAIN

At the decoder side, we try to obtain an estimate of each bit of the message, $\widehat{m_k}$, such that the probability of error $P_e = P(\widehat{m_k} \neq m_k)$ is minimized. To achieve this goal we employ the ML decoder with the hypothesis that the message bit has equal probability [16], i.e., $P(m_k = -1) = P(m_k = +1) = 1/2$. The ML approximation of the $\widehat{m_k}$ can be expressed as:

$$\widehat{m_k} = \text{argmax}\, f_Y(y|\, m_k, s, \alpha) \tag{7}$$

where $f_Y(y|m_k, s, \alpha)$ denotes the conditional PDF distribution of y when knowing m_k, s, and α. It is obvious that the ML performance is highly dependent on the distribution of the host signal and that is the main reason for proposing the Weibull distribution for the SVD domain in the previous section. The ML decoder for binary information hiding could be expressed by using the likelihood ratio rule. For this case the ML decoder decides $\widehat{m_k} = +1$ if

$$z = \frac{f_Y(y|\, m_k=+1)}{f_Y(y|\, m_k=-1)} > 1. \tag{8}$$

Depending on the transform domain used for embedding the message the PDF of the host signal can be different. In practice, due to different desired properties, various transform domains could be used for information hiding. Derivation and performance analyses of the ML decoder for SS embedding require the distribution of the host signal in a specific domain. Next, the ML decoder for the SS scheme in SVD domain is derived.

After introducing the SS embedding scheme (5) for information hiding in the SVD domain and the vector θ defined in (6), we can devise the optimal ML decoder using the distribution of the host signal. The joint PDF of the host data is computing, considering the distribution given in (8) and the independent and identical (iid) distribution of the SVs, as:

$$f_X(x;\, \tau, \gamma) = \exp\left\{-\sum_{i=1}^{L}\left(\frac{|x_i|}{\tau_i}\right)^{y_i}\right\} \prod_{i=1}^{L}\left[\frac{y_i}{\tau_i^{y_i}}(|x_i|)^{y_i-1}u(x_i)\right]. \tag{9}$$

Referring to (8), the ML decoder based on the joint PDF of the host decides $\widehat{m_k} = \pm 1$ based on the sign of the test statistic represented as

$$\text{sign}(z) = \text{sign}\left\{\frac{\exp\left\{-\sum_{i=1}^{L}\left(\frac{|y_i - s_i\cdot\alpha|}{\tau_i}\right)^{y_i}\right\} \prod_{i=1}^{L}\left[\frac{y_i}{\tau_i^{y_i}}(|y_i - s_i\cdot\alpha|)^{y_i-1}u(y_i - s_i\cdot\alpha)\right]}{\exp\left\{-\sum_{i=1}^{L}\left(\frac{|y_i + s_i\cdot\alpha\cdot m|}{\tau_i}\right)^{y_i}\right\} \prod_{i=1}^{L}\left[\frac{y_i}{\tau_i^{y_i}}(|y_i + s_i\cdot\alpha\cdot m|)^{y_i-1}u(y_i + s_i\cdot\alpha)\right]}\right\}. \tag{10}$$

Investigating the test statistic of the ML decoder in the DFT magnitude domain reveals that the bit information amplitude as well as the PDF parameters should be provided at the receiver side. The proposed decoder is error free for both cases of the bit message, i.e., if $m = 1$ and there is one coefficient with $y_i + s_i\alpha < 0$ at the decoder side, we can see that the test statistic in (10) goes to infinity and thus the decoder decides $\widehat{m_k} = +1$. Likewise, for the other case where at the decoder side there is one coefficient with $y_i + s_i\alpha < 0$, the test statistic in (10) goes to minus infinity and thus the decoder decides $\widehat{m_k} = -1$.

The test statistic employed for decoding is modeled as Gaussian random variable since is the sum of L random variables, we assume independent host signal samples and of signature codes ($s_i \in \{\pm 1\}$ and $P(s_i = -1) = P(s_i = +1) = 1/2$) are available at the decoder side. Then, the conditional PDFs of the test statistic are expressed as

$$\begin{cases} f_Z(z|\, m_k = +1) = \mathcal{N}(\mu_z, \sigma_z^2) \\ f_Z(z|\, m_k = -1) = \mathcal{N}(-\mu_z, \sigma_z^2) \end{cases} \tag{11}$$

where μ_z and σ_z^2 denotes the mean and variance of the test statistic. Thus the probability of error can be expressed as

$$P_e = \frac{1}{2} erfc\left(\sqrt{\frac{\text{WIR}}{2}}\right) = \frac{1}{2} erfc\left(\sqrt{\frac{m_z^2}{2\sigma_z^2}}\right) \tag{12}$$

where erfc(y) $= \frac{2}{\text{sqrt}(\pi)} \int_y^{\infty} e^{-t^2}\, dt$ is the complementary error function and WIR $= \frac{m_z^2}{2\sigma_z^2}$ represents the watermark to interference ratio.

6. EVALUATION AND RESULTS

We conduct a set of experiments on 100 test images, of size 512×512 pixels taken from the IR database available at [32], to illustrate the performances of the proposed data hiding scheme. The block size is set to 8×8 in which we hide one bit of the message; thus the total size of the message is 4096 bits. From each block 7 SVs are chosen (we discard the first SV) for the information hiding and the bit amplitude is α = 5.0. Our results are based on 100 simulation runs with using different signature codes generated via the secret key.

The experiments aim to validate the error probability when using the adjusted ML decoder for the SS embedding framework. In Fig. 2 both the empirical and theoretical results are illustrated, where the bit-error-rate (BER) is plotted against document-to-watermark ratio (DWR) which is equal to

$$DWR = 10 \cdot \log \frac{\sigma_x^2}{D} = 20 \cdot \log \frac{\sigma_x}{\alpha}. \tag{7}$$

It is worth pointing out that the values of the BER are averaged along 100 images. From Fig. 1 we can observe that the theoretical and empirical results match closely, which confirms the behavior of the error probability.

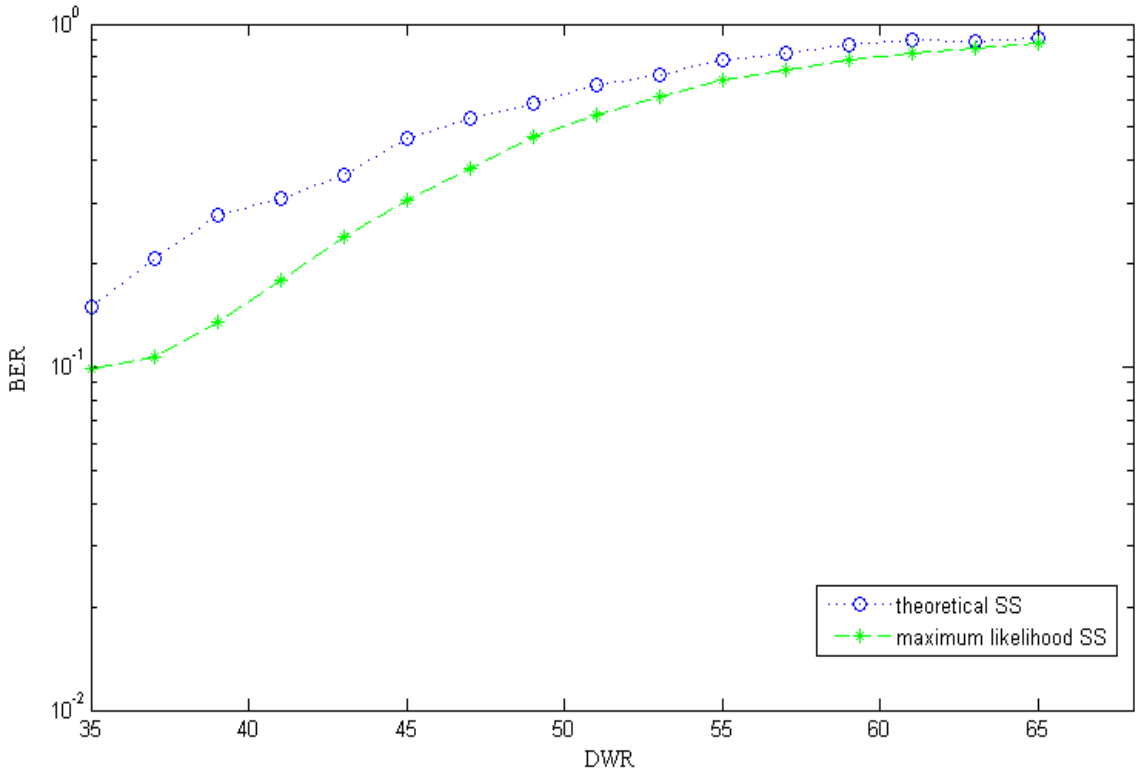

Fig. 1. The average bit error rates versus DWR for the ML decoder when a message of 4096 bits length is inserted into the SVD domain of 100 test images. For comparison, the theoretical SS performances are also provided.

In order to illustrate that the proposed modified SS scheme in the SVD domain always lead to positive watermarked coefficients, the histogram plots of the watermarked coefficients for the proposed modified scheme is provided in Fig. 2. It could be seen that, as we expected, all coefficients are positive, supporting the intuitive rationale behind using the modified embedding schemes.

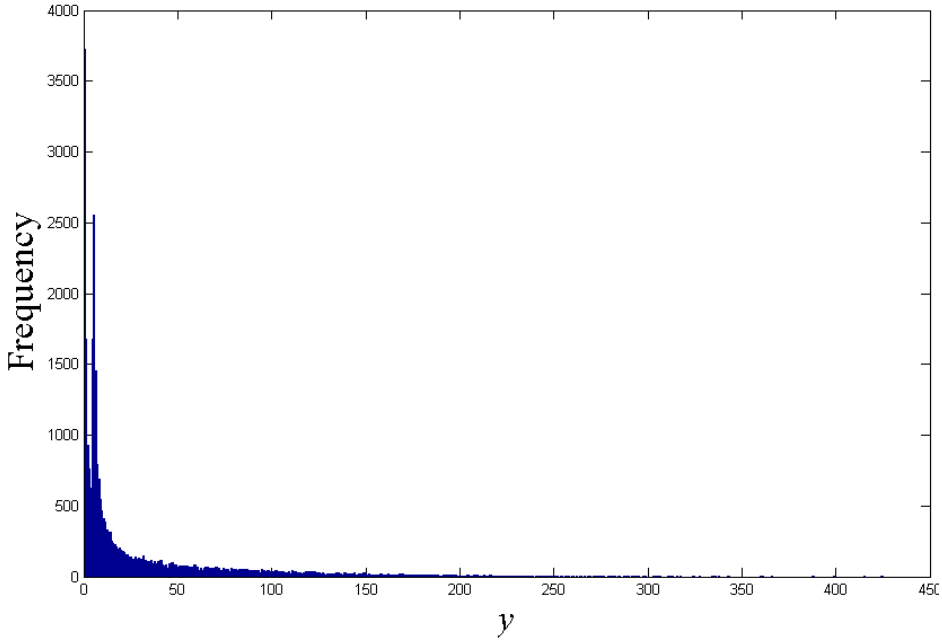

Fig. 2. Histogram of the watermarked coefficients (i.e., the SVs) using the modified SS embedding rule. Note that modified SS scheme in the SVD domain always lead to positive watermarked coefficients.

To verify whether the Weibull distribution is a valid assumption for the SVs, we estimate the PDF of the coefficients based on the Weibull distribution and report empirical results for 100 images. Fig. 3 shows that the Weibull distribution assumption for the SVs is valid since the empirical and the theoretical PDFs of the second SV for 100 images are in close agreement.

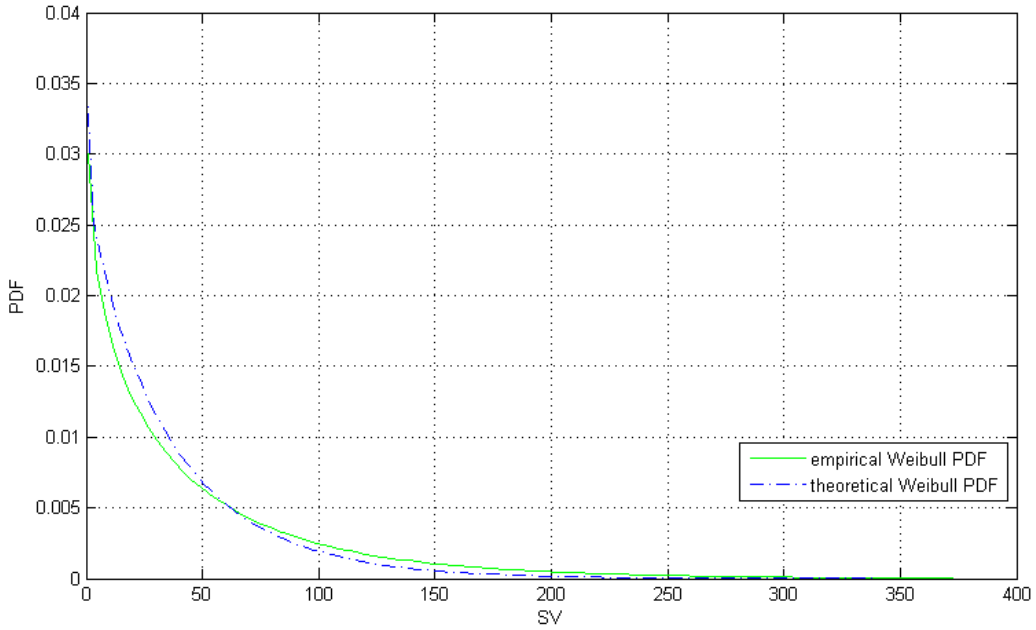

Fig. 3. The estimated and theoretical Weibull PDF of the second SV for 100 images acquired from the IR database [32].

7. CONCLUSION

In this paper the optimal decoder for additive spread spectrum data hiding were analyzed for the IR images. Generally, we proposed a rigorous decoding analysis scheme of additive spread spectrum data hiding when the information bit is

embedded into the SVs of the SVD domain. We assumed for the SVs the Weibull distribution for deriving the ML decoders in the SVD domain.

The theoretical error analysis of SS embedding in the SVs of the SVD domain was derived. Simulation results showed that, when the watermark amplitude is available at the decoder side, data hiding in the SVs of the SVD domain could yield good decoding performances.

REFERENCES

[1] N.J.W. Morris, S. Avidan, W. Matusik, and H. Pfister, "Statistics of Infrared Images," Proc. CVPR 1(7), 17-22 (2007).

[2] I. J. Cox, M. L. Miller, J.A. Bloom, J. Fridrich, and T. Kalker. [Digital Watermarking and Steganography], 2nd ed. Morgan Kaufmann Publishers Inc. San Francisco, CA, USA, (2008).

[3] B. Chen, and G. Wornell,"Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," IEEE Trans Inf Theory 47(4), 1423–1443 (2001).

[4] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: theory and practice," IEEE Transactions on Signal Processing 53(10), 3976-3987 (2005).

[5] J.J Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding," IEEE Trans Signal Processing 51(4), 1003–1019 (2003).

[6] A.K. Mairgiotis, and N.P. Galatsanos, Y. Yang, "New additive watermark detectors based on a hierarchical spatially adaptive image model," IEEE Trans Inf Forensics Security 3(1), 29-37 (2008).

[7] J Cannons, and P Moulin, "Design and statistical analysis of a hash-aided image watermarking system," IEEE Trans Image process. 13(10), 1393-1408 (2004).

[8] A Valizadeh, and ZJ Wang, "A framework of multiplicative spread spectrum embedding for data hiding: performance, decoder and signature design," in Proc Global Communications, 1–6 (2009).

[9] HS Malvar, and DA Florencio, "Improved spread spectrum: a new modulation technique for robust watermarking," IEEE Trans Signal Processing 51(4), 898–905 (2003).

[10] J Delhumeau, T Furon, NJ Hurley, and GC Silvestre, "Improved polynomial detectors for side-informed watermarking," in Proc SPIE 5020, 311–321 (2003).

[11] A Valizadeh, and ZJ Wang, "Correlation-and-bit-aware spread spectrum embedding for data hiding," IEEE Trans Inf Forensics Security 6(2), 267–282 (2011)

[12] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "Optimum decoding and detection of multiplicative watermarks," IEEE Transactions on Signal Processing 51, 1118-1123 (2003).

[13] J Zhong, and S Huang, "Double-sided watermark embedding and detection," IEEE Trans Inf Forensics Secur. 2(3), 297–310 (2007) .

[14] W Liu, L Dong, and W Zeng, "Optimum detection for spread-spectrum watermarking that employs self-masking," IEEE Trans Inf Forensics Secur. 2(4), 645–654 (2007).

[15] P. Premaratne, and C. C. Ko, "A novel watermark embedding and detection scheme for images in DFT domain," Proc. of 7th International Conference on Image Processing 2, 780-783 (1999).

[16] N Merhav, and E Sabbag, Optimal watermark embedding and detection strategies under limited detection resources. IEEE Trans Inf Theory. 54(1), 255–274 (2008).

[17] C Lin, M Wu, JA Bloom, I Cox, M Miller, and Y Lui, "Rotation, scale, and translation resilient watermarking for images," IEEE Trans Image Processing 10(5), 767–782 (2001).

[18] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transaction on Image Processing 6(12), 1673-1687 (1997).

[19] HW Kim, D Choi, H Choi, and T Kim, "Selective correlation detector for additive spread spectrum watermarking in transform domain," Signal Process. 90(8), 2605–2610 (2010).

[20] H. Inoue, A. Miyazaki, and T. Katsura, "Wavelet-based watermarking for tamper proofing of still images," in Proc. of International Conference on Image Processing 2, 88-91 (2000).

[21] X. Xiaoqing, W. Jingzhong, and Li Dan, "A Chaotic Sequence Watermarking Algorithm for Infrared Image," Proc Information Engineering and Computer Science, 1-4 (2010).

[22] A. Basso, F. Bergadano, D. Cavagnino, V. Pomponiu, and A. Vernone, "A Novel Block-based Watermarking Scheme Using the SVD Transform," Algorithms 2(1), 46-75 (2009).

[23] V. Pomponiu, and D. Cavagnino, "Security analysis of SVD-based watermarking techniques," International Journal of Multimedia Intelligence and Security 2(2), 120-145 (2011).

[24] JR Hernandez, M Amado, amd F Perez-Gonzalez, "DCT-domain watermarking techniques for still images: detection performance analysis and a new structure," IEEE Trans Image Process. 9(1), 55–68 (2000).

[25] R.M. May, "Simple mathematical models with very complicated dynamics." Nature 261(5560), 459-467 (1976).
[26] A. S. Lewis, and G. Knowles, “Image compression using the 2-D wavelet transform,” IEEE Trans. Image Processing 1(2), 244-250 (1992).
[27] Y. Zhao, Z. Fan, and M.E. Hoover, "Frequency domain infrared watermarking for printed CMYK image," Proc. ICIP, 2725-2728 (2011).
[28] T. Yamada, S. Gohshi, and I. Echizen, “IR Hiding: A Method to Prevent Video Re-shooting by Exploiting Differences between Human Perceptions and Recording Device Characteristics” in IWDW, LNCS 6526, 280–292 (2011).
[29] T. Yamada, S. Gohshi, and I. Echizen, “IR Hiding: Method to Prevent Re-recording Screen Image Built in Short Wavelength Pass Filter Detection Method Using Specular Reflection,” Digital Forensics and Watermarking, LNCS 7128, 111-125 (2012).
[30] I. Echizen, T. Yamada, and S. Gohshi, “IR Hiding: Use of Specular Reflection for Short-Wavelength-Pass-Filter Detection to Prevent Re-recording of Screen Images,” T. Data Hiding and Multimedia Security X, LNCS 8948, 38-54 (2015).
[31] L. N. Trefethen, and B. David, [The Singular Value Decomposition], Numerical Linear Algebra, SIAM, 25-31 (1997).
[32] http://www.dgp.toronto.edu/~nmorris/data/IRData/.